Lobachevskii Journal of Mathematics 2016 vol.37 N6, pages 768-776

Some new platforms for algebraic cryptography and one method of increasing the security

Gaynullina A., Tronin S.
Kazan Federal University, 420008, Kremlevskaya 18, Kazan, Russia

Abstract

© 2016, Pleiades Publishing, Ltd.In this paper we discuss the possibility of using the categorical groupoids and the commutative operads in algebraic cryptography. Also, we introduce a general method of constructing the cryptographic protocols on the algebraic platforms. Under certain reasonable assumptions, this method allows to get a new sufficiently cryptographically strong protocol using several other protocols. Moreover, each of these protocols can be vulnerable. Sufficient cryptographic security means that the protocol will be protected for some preassigned finite time.

http://dx.doi.org/10.1134/S1995080216060123

Keywords

algebra over an operad, Algebraic cryptography, commutative operad, computational complexity, cryptographic protocol, key exchange, masked group, masked operad, platform, secret key, security, tropical semiring